Network Security Homework – 2

Srinivas Piskala Ganesh Babu – spg349 and N13138339

Homework #2 – CS6823 – Network Security

1. [16 pts] What's the difference between:

a. Plaintext vs. Ciphertext

Plain text:

- Plain text is data in **unencrypted, human readable** format
- Plain text can be **compromised by anyone** in possession and knowing the language the message is made up of.

Cipher text:

- Cipher text is data **or message in encrypted form** usually with **some method and a key**, it is **unreadable text**, it maybe human readable format but is **in meaning less state**
- It is **meaning less without the key**, hence message can't be compromised with possession unless the key is obtained.

b. Encryption vs. Decryption

Encryption:

- It is the process of **converting a plain text to a cipher text or encrypted text or meaning less state** with the help of a key and any method
- It helps to **protect the message (Both Confidentiality and Integrity)**
- It **inputs plain text** and **outputs an encrypted or unreadable form** of the same message (hiding it with a key)

Decryption:

- It is the process of **converting a cipher text or encrypted text or meaning less state messages into human readable messages**.
- It helps in **obtaining the human readable** message from the encrypted or meaning less form.
- It **inputs encrypted or cipher** text and **outputs plain text or human readable** form of message

c. Symmetric Key Cryptography vs. Asymmetric Key Cryptography

Symmetric Key Cryptography:

- **The Same Key** is used to Encrypt and Decrypt the message
- The process involves **only one Key**
- The communication is **compromised if the key** is known
- Both the Sender and Receiver should possess the key which makes it **difficult to share the key**

Asymmetric Key Cryptography:

- **Two different keys** are used to Encrypt and Decrypt the message
- The process involves **2 different keys** – A public and private key
- The connection **is not compromised unless the private key is known**. One of the key called public key is shared which cannot be used to compromise the communication
- **Sharing the public key is an easy way** as only the unshared private key can be used to decrypt the message

d. Encryption Algorithm vs. Encryption Key

Encryption Algorithm:

- **Algorithm is a method used to perform the encryption** with a key
- An algorithm **elaborates steps needed** to be done with the key and message to encrypt it or decrypt it
- For an algorithm selected, it is required to stick to the rules and steps of the algorithm only

Encryption Key:

- Is the Entity that is used to **perform an encryption based on any algorithm**
- **A Key is required to provide the output,** encrypt and decrypt the plaintext and cipher text respectively
- **A Key is mandatory** to perform encryption and decryption of any message.
- **There can be a number of keys** for any selected algorithm.

2. [6 pts] Describe Cipher-text only attack, Known-plaintext attack, and Chosen-plaintext attack.

***Cipher text Only Attack:**

- Identify the structure of cipher and guess the Key that may be used. (Number of Bits of cipher, Length)

- Use the Guessed Keys and try to **decrypt the cipher text with various keys unless a meaningful plain text** is obtained

Cipher Text + (Random or Guessed Keys) -> Unless a Meaning full text is obtained

***Known- Plain Text Attack:**

- The Cipher Text and Plain Text is obtained

- Information regarding the **Key and the Algorithm** is obtained by brute forcing various values of keys and methods.

Cipher Text + Plain Text -> Key or Algorithm Data matches the encrypt and decrypt

***Chosen-Plaintext Attack:**

- Cipher text is obtained

- Randomly chosen or guessed plain text are used to encrypt with a chosen key and algorithm unless the cipher text matches the plain text

Chosen Plain Text + Encrypt (Algo + Key) => Unless it matches the Cipher text

3. [6 pts] Why is block ciphers "mode of operations" required for block ciphers such as AES

*The block cipher mode of operations is required so **that repeated messages don't produce the same cipher text.**

*The **blocks that are same don't produce the same cipher text** rather than a different one to protect the cipher text from being analyzed to be repetition of any message

* To perform **a mixture in the blocks of message** leading to more ambiguity and encryption standards (**Like shuffling a deck of cards**)

4. [6 pts] Encrypt "NYU" with a Julius Caesar's Cipher of key -4 (negative 4).

Plain Text : M N O P Q R S T U V W X Y Z A B and Key = -4

Cipher Txt : I J K L M N O P Q R S T U V W X Y Z

NYU ===== JUQ

Network Security Homework – 2

Srinivas Piskala Ganesh Babu – spg349 and N13138339

5. **[6 pts] Decrypt your result from the previous question to obtain the plaintext message. Show work.**

   Cipher Text: I J K L M N O P Q R S T U V W X Y Z   Key = +4
   Plain Text : M N O P Q R S T U V W X Y Z A B C D

   JUQ == NYU

6. **[6 pts] Encrypt "cyber"**

   ```
   Plaintext:  abcdefghijklmnopqrstuvwxyz
   Ciphertext: mnbvcxzasdfghjklpoiuytrewq
   ```

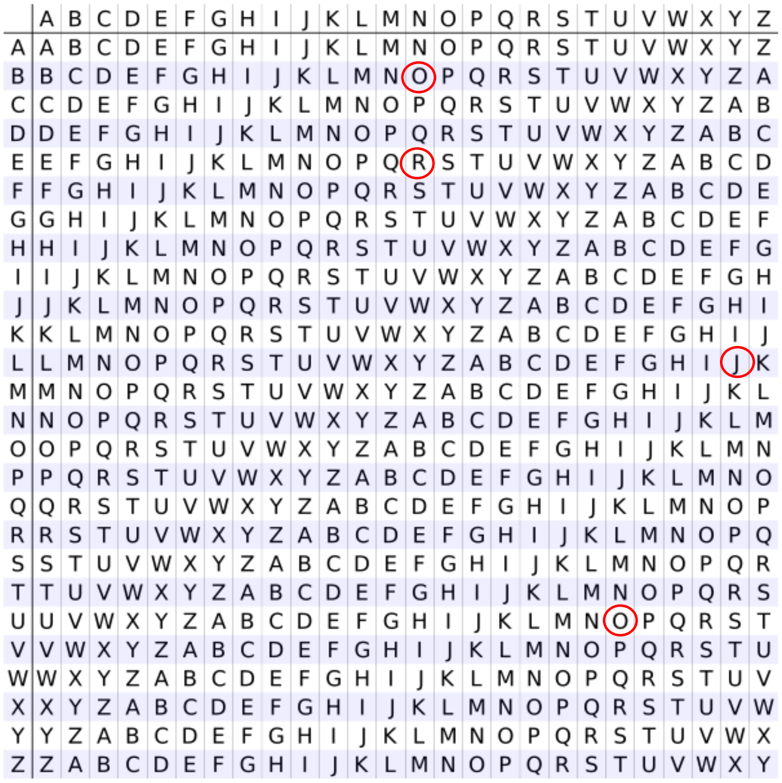
   Cyber == bwnco

7. **[6 pts] Decrypt "jcuicb"**

   ```
   Plaintext:  abcdefghijklmnopqrstuvwxyz
   Ciphertext: mnbvcxzasdfghjklpoiuytrewq
   ```

   Jcuicb === netsec

8. **[10 pts] Using the Vigenère Cipher with the key "NYU", encrypt "BLUE". Note: on an exam, you may be asked to perform this without being given the table.**



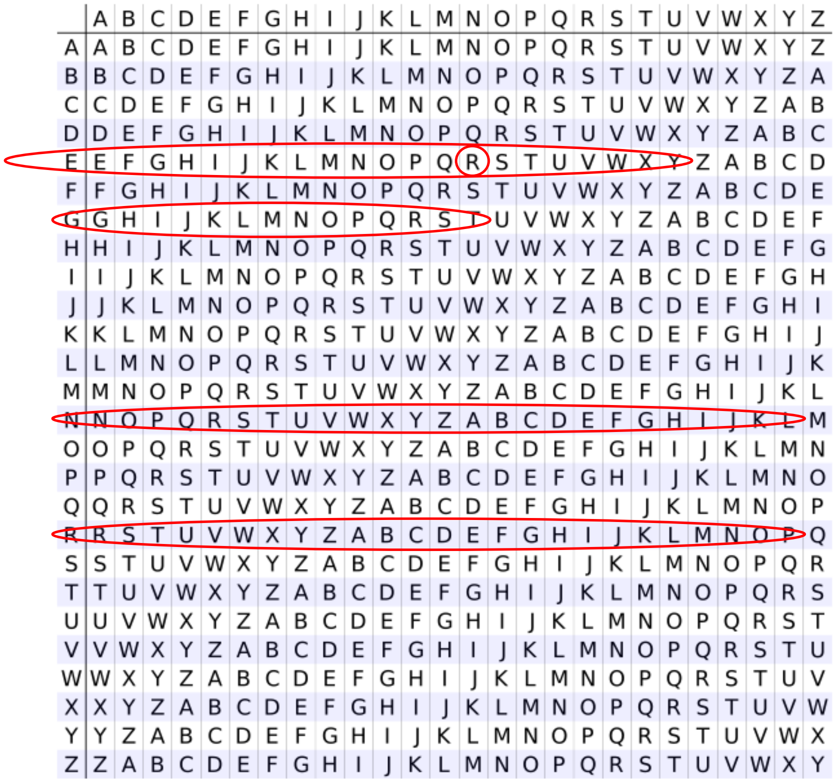
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

BLUE + NYU === OJOR

Network Security Homework – 2

Srinivas Piskala Ganesh Babu – spg349 and N13138339

9. [10 pts] Using the Vigenère Cipher, decrypt “TPYRL” using the key “NYU”.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

TPYRL + NYU = GREEN

10. [10 pts] Compute 77^7 mod 15 without a calculator. Write out your calculations.

77^7 mod 15 = 8

- 77^1 mod 15 = 2
- 77^2 mod 15 = (77^1 mod 15 * 77^1 mod 15) mod 15 = 4 mod 15 = 4
- 77^3 mod 15 = (77^1 mod 15 * 77^2 mod 15) mod 15 = 8 mod 15 = 8
- 77^4 mod 15 = 4*4 mod 15 = 1
- 77^7 mod 15 = (77^3 mod 15 * 77^4 mod 15) mod 15 = 8*1 mod 15 = 8

Use the following block cipher scheme for rest of the questions.

Input	**Output**
000	111
001	110
010	100
011	101
100	011
101	000
110	001
111	010

Network Security Homework – 2

Srinivas Piskala Ganesh Babu – spg349 and N13138339

11. **[6 pts] Without using Cipher Block Chaining (CBC), what's the Ciphertext for 011110001100?**

    011 - 101
    110 - 001
    001 - 110
    100 – 011

    The Cipher Text is **101001110011**

12. **[6 pts] Using CBC and an IV=101, what's the Ciphertext for 011110001100?**

    CT1 = E(IV XOR PT1) = E(101 xor 011) = E(110) = 001
    CT2 = E(CT1 XOR PT2) = E(001 xor 110) = E(111) = 010
    CT3 = E(CT2 XOR PT3) = E(010 xor 001) = E(011) = 101
    CT4 = E(CT3 XOR PT4) = E(101 xor 100) = E(001) = 110

    ⇨ **001010101110**

13. **[6 pts] Decrypt your answer in the previous question. Show work.**

PT1 = D(CT1) XOR IV = D(001) XOR 101 = 110 XOR 101 = 011
PT2 = CT1 XOR D(CT2) = 001 XOR D(010) = 001 XOR 111 = 110
PT3 = CT2 XOR D(CT3) = 010 XOR D(101) = 010 XOR 011 = 001
PT4 = CT3 XOR D(CT4) = 101 XOR D(110) = 101 XOR 001 = 100

⇨ **011110001100**